Amendments to the Specification:

Please replace the paragraph extending from page 6, lines 15-21, with the following amended paragraph:

-- This invention provides for a novel encryption system and method that may encrypt all of the transmitted and received data packets on the data link layer without collisions on the Initialization Vector (IV). In the encryption system and method of the present invention a new final key value is generated and may be applied to every transmitted and received data packet. The encryption system and method of one advantageous embodiment entails a three phase algorithmic process for generating a final ~~secret~~ key.--

Please replace the paragraph extending from page 7, lines 13-21, with the following amended paragraph:

-- Another aspect of the present invention is defined by a method for generating a key for data encryption in a communication network that includes the steps of generating an Initialization Vector (IV) value, combining a first secret key with the IV value to result in an intermediate value and thereafter permutating the intermediate value. The first secret key may be generated as described above by combining a predefined ~~predetermined~~ secret key with a user-specific MAC address to result in an intermediate value, combining this intermediate value with predefined key change information and thereafter transforming the combination of the intermediate value and the predefined key change information, such as by hashing.--

Please replace the paragraphs extending from page 7, line 27 to page 8, line 21 with the following amended paragraphs:

-- In another aspect of the present invention a method for generating a key for data encryption in a communications network is defined by the steps of calculating a first secret key utilizing predefined key change information, determining if the key change information has repeated and differently processing the first secret key to generate the key for data encryption in instances in which the key change information has repeated than in instances in which the key

change information has not repeated. For example, the first secret key may undergo a bitwise shift in instances in which the key change information has not repeated. The step of calculating a first secret key may be performed as described above and, as such, may involve the steps of selecting a predefined ~~predetermined~~ secret key, combining the predefined ~~predetermined~~ secret key with a user-specific MAC address to result in a first intermediate value, combining the first intermediate value with predefined key change information, transforming the combination of the first intermediate value and the predefined key change information, such as by hashing, to generate a temporary key, combining the temporary key and an IV value and permutating the combination of the temporary key and the IV value to result in the first secret key.

By combining the various aspects of the encryption process, a method is provided according to one embodiment of the present invention which includes the steps of selecting a first secret key, generating a first temporary key based upon a combination of the first secret key with at least a portion of the user-specific MAC address and further based upon predefined key change information followed by hashing. A second temporary key is then generated based upon a combination of the first temporary key and an IV value. After determining if the predefined key change information has been repeated, the key for data encryption may be generated based upon the second temporary key and the determination of whether the predefined key change information has repeated.--

Following the paragraph which ends at page 8, line 26 and prior to the section titled "BRIEF DESCRIPTION OF THE DRAWINGS", please add the following paragraph:

-- In an exemplary embodiment, if it is determined that the data is originally encrypted in accordance with a predetermined encryption technique, the data may be decrypted prior to encrypting the data transmitted via the communication network with the final key.--

Please replace the paragraph extending from page 9, lines 23-25, with the following amended paragraph:

-- Figure 7 is a block diagram of the first phase of the encryption algorithm that results in generation of a first temporary ~~secret~~ key, in accordance with an embodiment of the present invention.--

Please replace the paragraph extending from page 9, lines 29-31, with the following amended paragraph:

-- Figure 9 is block diagram of the second phase of the encryption algorithm that results in generation of a second temporary ~~secret~~ key, in accordance with an embodiment of the present invention.--

Please replace the paragraph extending from page 11, lines 20-28, with the following amended paragraph:

-- The novel encryption/decryption system includes a data packet analyzer **22** that analyzes data packets to determine if encryption/decryption is appropriate, an encryptor **24** that encrypts the data packets according to the three phase encryption process discussed at length below, an initialization vector generator **26** that generates an initialization vector and a decryptor **28** that uses a predefined secret ~~public~~ key to decrypt messages coming from the physical layer of network. The encryption/decryption system **20** is in communication with a memory device **50** that stores relevant information, such as hash tables, timing values, MAC addresses, etc., that are implemented in the algorithms of the encryption system.--

Please replace the paragraph extending from page 14, lines 3-25, with the following amended paragraph:

-- Figure 6 is a simplified flow diagram that illustrates the three-phase nature of the encryption algorithm of one advantageous embodiment of the present invention. While the system and method of the present invention will be described in terms of encryption, the system and method applies equally to decryption as will be apparent to those skilled in the art. Prior to beginning the encryption process, data packets are first analyzed, at step **140**, as described above to determine the need for encryption. After the data packets have been analyzed the first phase of the encryption process ensues, at step **150**. The first phase of the algorithm involves changing the selected shared secret key by implementing a bitwise exclusive OR (XOR) operation, a modification routine and a hashing routine to result in a first temporary ~~secret~~ key. After the first temporary ~~secret~~ key has been established the second phase commences, at step **160**, with the

second phase of the algorithm involving bitwise XORing of the first temporary ~~secret~~ key from phase one and an IV value. The result of the bitwise XOR process undergoes a permutation process resulting in generation of a second temporary ~~secret~~ key. After the second temporary ~~secret~~ key has been established the third phase of the algorithm is initiated, at step **170**. The third stage of the algorithm involves modification of the second temporary ~~secret~~ key if a determination is made that the key changing information (described below) has been repeated, thereby indicating that a certain number of secret keys have been generated with the key changing information being modified in a predefined manner from key to key. A final key value results from either the modification or the determination that no modification is required. Each of these phases is described in much greater detail below.--

Please replace the paragraphs extending from page 16, lines 5-14, with the following amended paragraphs:

-- Returning to Figure 7, after the modification process is completed the first phase of the encryption algorithm performs a hashing operation at step **240**. The hashing operation is conducted using a conventional hash table comprised of asynchronous non-linear values, such as S-Box. The S-Box hash table is well known by those of ordinary skill in the art, although other hash functions can be employed if desired. The result of the hashing operation is a first temporary ~~secret~~ key.

Figure 9 is a block diagram of the second phase of the encryption algorithm, in accordance with an embodiment of the present invention. At step **300**, the first temporary ~~secret~~ key from the first phase of the encryption algorithm is obtained. At step **310**, the second phase of the encryption algorithm obtains an IV value.--

Please replace the paragraphs extending from page 16, line 27 to page 17, line 31, with the following amended paragraphs:

-- Referring again to the second phase block diagram of Figure 9, at step **320** a bitwise XOR operation is performed on the first temporary key from phase one and the IV value. The result of the bitwise XOR then undergoes, at step **330**, permutation processing. In one embodiment of the invention, permutation processing involves two separate processes. First, an

exchange between the upper 8 bits and the lower 8 bits in the 16-bit IV value is undertaken to provide for a wider range of keys. Second, the 128-bit key that results from the bitwise XOR operation and the exchange of upper and lower bits becomes the address of the Substitution Box (S-Box) and its value is outputted. This output is then rotated by shifting right by 1 bit, resulting in the output of the permutation process, referred to herein as a second temporary ~~secret~~ key.

Figure 11 is a flow diagram of the third phase of the encryption algorithm, in accordance with an embodiment of the present invention. In the third phase of the encryption algorithm, further modification of the secret key is performed if it is determined that the key changing information is repeated. When the key generation space is exhausted due to the 8-bit size of the key changing information, the key changing information repeats. At step **400,** a key change information variable is analyzed to determine if the key changing information is repeated. The key change information serves as a counter that is incremented by 1 for each different secret key that is generated and is then reset to 0 once the key changing information repeats. As a result of the key change information having 8 bits in the illustrated embodiment, repetition of the key change information is determined by checking the key change information value to see if it equals 0xFF, thereby indicating that 256 secret keys have been generated without having the key change information repeat. If it is determined in step **400** that the key change information has ~~not~~ repeated by the key change information value equaling ~~being some value less than~~ 0xFF, then modification of the secret key is required by shifting or rotating the secret key to the right by one bit as shown in the lower portion of Figure 8 and in step **430**. The key change information value is incremented by one ~~as shown in step **420**~~. The secret key that results from the rotation to the right is deemed the final key value, which is used to encrypt a data packet. In contrast, if a determination is made that the key change information has repeated as indicated by the key change information value being some value less than ~~equaling~~ 0xFF, then the second temporary ~~secret~~ key is considered the final key value. In this case, the key change information value is also set to zero to start the process over. In either instance, the final key value is used as the "seed" for the Pseudo Random Number Generator (PRNG), which performs the encryption algorithm.--